MATH 844: HOMEWORK 8, DUE MAR 30.

8. Let E be an elliptic curve over $\mathbf{F}_q$.

(a) Show that $E(\mathbf{F}_q) \cong \mathbf{Z}/m \times \mathbf{Z}/mn$ for some integers $m, n \geq 1$ with $\gcd(m, q) = 1$.

(b) With the notation of (a), show that $q \equiv 1 \pmod{m}$.

(c) Suppose that q is a prime ≥ 5 and that E is supersingular. Show that $m = 1$ or 2. If $q \equiv 1 \pmod{4}$, prove that $m = 1$.